ABSTRACT OF THE DISCLOSURE

METHOD AND SYSTEM FOR SECURE SERVER-BASED SESSION MANAGEMENT USING SINGLE-USE HTTP COOKIES

A methodology for providing secure session management is presented. After a single-use token has been issued to a client, it presents the token, and the server may identify the client based upon the presented token. However, the token may be used only once without being refreshed prior to re-use, thereby causing the token to be essentially reissued upon each use. The token comprises a session identifier that allows the issuer of the token to perform session management with respect to the receiving entity. Tokens can be classified into two types: domain tokens and service tokens. Domain tokens represent a client identity to a secure domain, and service tokens represent a client identity to a specific service. A domain token may be used with any service within a domain that recognizes the domain token, but a service token is specific to the service from which it was obtained.